Technical Bulletin
Horizon 900 Security

OVERVIEW

The security for the ESTeem Horizon 900, like all network security, must be multi-layered. One level of security is never enough to make sure that data does not end up in the wrong hands. Please review the following security levels and decide what is the most appropriate for your network.

PROPRIETARY COMMUNICATION

The ESTeem Horizon 900 operates in the unlicensed 900 MHz frequency band. This frequency band does not comply with any "open" standards and no other manufacturer of wireless hardware can access the ESTeem network when either bridging between Ethernet networks or being used as a mobile client. This proprietary communication layer, in combination with the other security settings listed below, allow you as the user to reject wireless clients into the network if so desired.

The security level of the bridge communication link is configurable for 64-Bit WEP, 128-Bit WEP, TKIP and CCMP and is completely independent of the client access level or any other communication link level. For example, an ESTeem Horizon 900 can be configured for WPA Enterprise for client level access, communicate to another ESTeem Horizon 900 using a TKIP bridge link.

CCMP (AES 128/256-bit)

AES-CCMP (Advanced Encryption Standard-Counter Mode CBC-MAC Protocol) is the encryption algorithm used in the IEEE 802.11i and WPA-2 security protocols. This encryption standard uses either 256 or 128 bit-AES block cipher and CCMP technique to ensure the highest level of security and integrity available on a wireless network. AES-CCMP incorporates two sophisticated cryptographic techniques (counter mode and CBC-MAC) and adapts them to Ethernet frames to provide a robust security protocol between the mobile client and the access point. AES itself is a very strong cipher, but counter mode makes it difficult for an eavesdropper to spot patterns, and the CBC-MAC message integrity method ensures that messages have not been tampered with. The ESTeem Horizon 900 is compatible as either an Access Point or mobile client using WPA2 security systems.

Wi-Fi Protected Access 2 with Preshared Key (WPA2 PSK**)**
WPA2 PSK uses a common passphrase (preshared key) between the Access Point (AP) and the client to begin a secure communication session. This passphrase must be entered exactly the same in both the Access Point and the client. This passphrase is used to authenticate communication session between the AP and client to begin the secure wireless networking session.

Wi-Fi Protected Access 2 with Enterprise Server (WPA2 Enterprise)
Like WPA2 PSK, WPA2 Enterprise verifies the authenticity of the Access Point and client, but uses an 802.1x backend authentication server handling the authentication decision. The most commonly type of authentication server is a RADIUS server. The ESTeem Horizon 900 can be configured to operate with an established RADIUS server on the network.

In an ESTeem Horizon 900 wireless network, WPA2 is server/client relationship between an ESTeem Horizon 900 configured in a Station mode (Etherstation, Station Router or Station Masquerade) and an ESTeem Horizon 900 configured in an Access Point mode (AP Bridge, AP Router or AP Masquerade). The scope of WPA2 Enterprise is limited in use to this mobile client configuration only. The security level on the Bridging layer is configured separately.

Technical Bulletin
Horizon 900 Security

WPA

Wi-Fi Protected Access with Preshared Key (WPA PSK)
WPA, which uses 802.1x, was introduced in 2003 to improve on the authentication and encryption features of WEP. All authentication is handled within this access point device. WPA has two significant advantages over WEP:

1. An encryption key differing in every packet. The TKIP (Temporal Key Integrity Protocol) mechanism shares a starting key between devices. Each device then changes their encryption key for every packet. It is extremely difficult for hackers to read messages even if they have intercepted the data.
2. Certificate Authentication (CA) can be used, blocking a hacker posing as a valid user.

Wi-Fi Protected Access with Enterprise Server (WPA Enterprise)
Like WPA PSK, WPA Enterprise verifies the authenticity of the Access Point and client, but uses an 802.1x backend authentication server handling the authentication decision. The most commonly type of authentication server is a RADIUS server. The ESTeem Horizon 900 can be configured to operate with an established RADIUS server on the network.

WPA is server/client relationship from a software driver on a computer's wireless LAN (WLAN) card to an Access Point. The scope of WPA is limited in use to this configuration only. The ESTeem Horizon 900 can support WPA Enterprise and PSK as an Access Point, but the level of security on the Bridging layer is configured separately.

In an ESTeem Horizon 900 wireless network, WPA is server/client relationship between an ESTeem Horizon 900 configured in a Station mode (Etherstation, Station Router or Station Masquerade) and an ESTeem Horizon 900 configured in an Access Point mode (AP Bridge, AP Router or AP Masquerade). The scope of WPA PSK and Enterprise is limited in use to this mobile client configuration only. The security level on the Bridging layer is configured separately.

128-BIT WEP

The 128 WEP uses a particular algorithm called RC4 encryption to encode and decode traffic that is based on a 104-bit encryption key and a 24-bit Initialization Vector (IV). RC4 starts with a relatively short encryption key (104 bits) that is expanded into a nearly infinite stream of keys to accompany the stream of packets.

The basic concept of RC4 is good, but the way it's implemented in WEP leaves it open to compromise. The researchers that test the integrity of the system usually focus on one piece of the implementation, the Initialization Vector (IV).

The IV (24 bits) is the algorithm component that's supposed to keep expanded keys from repeating. From the researcher's point of view, a high-volume access point is mathematically guaranteed to reuse the same key stream at least once a day. When this happens, it's called an IV collision this becomes a soft spot to enter the system.

The researchers aren't saying that it's easy to break into the system, or that it's being done on a regular basis, only that it is possible and that administrators should consider ways to reduce the possibility.

MASQUERADE MODES

The ESTeem Horizon 900 functions as a network firewall when configured in either the Access Point Masquerade or Client Masquerade modes. If access to the wired network is the greatest concern, place the ESTeem in the Masquerade mode and the wireless network will be completely isolated from the wired Ethernet network.

Technical Bulletin
Horizon 900 Security

INCREASING NETWORK SECURITY

The following are a few suggestions to help improve the overall security of your wireless network:

1. Enable the security. If you research all of the articles regarding hackers, they have gotten into the user's network due to the security not being enabled.

2. Make sure the keys are not reused in your company, since reuse increases the statistical likelihood that someone can figure the key out and change the default password on your access point or wireless router

3. Many access points allow you to control access based on the MAC address of the NIC attempting to associate with it. If the MAC address of your NIC isn't in the table of the access point, you won't associate with it. And while it's true that there are ways of spoofing a MAC address that's been sniffed out of the air, it takes an additional level of sophistication to spoof a MAC address. The downside of deploying MAC address tables is that if you have a lot of access points, maintaining the tables in each access point could be time consuming. Some higher-end, enterprise-level access points have mechanisms for updating these tables across multiple access points of the same brand.

4. If you're deploying a wireless router, think about assigning static IP addresses for your wireless NICs and turn off Dynamic Host Configuration Protocol (DHCP). If you're using a wireless router and have decided to turn off DHCP, also consider changing the IP subnet. Many wireless routers default to the 192.168.1.0 network and use 192.168.1.1 as the default router.

5. Only purchase wireless devices that have flashable firmware. There are a number of security enhancements that are being developed, and you want to be sure that you can upgrade your access point.

6. A simple security technique used by the military is to have the administrator periodically change the key for the system i.e. weekly, monthly, etc.